K

Page 1

UNITED STATES DISTRICT Court

DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation

Plaintiff and
Counterclaim-Defendant,
vs. No. 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation; and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs. /

DEPOSITION OF GEORGE KESIDIS

VOLUME I

DATE: May 25, 2006

TIME: 9:13 a.m.

LOCATION: DAY CASEBEER MADRID & BATCHELDER
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014

REPORTED BY: KAREN L. BUCHANAN
CSR No. 10772

Page 64

11:02:46 signature-based attack, would it be relevant to
11:02:46 claim 1?
11:02:48 MR. POLLACK: Objection. Vague and
11:02:51 ambiguous. Claim 1 of the '338?
11:02:52 MS. MOEHLMAN: Claim 1 of '338.
11:02:55 THE WITNESS: Claim 1 of '338. If a
11:02:57 component only used a significant-based attack, would
11:03:14 it be relevant to claim 1? Well, let me just -- in
11:03:17 answering that question, I'm going to have to stake
11:03:20 out an opinion of what "signature" is, what exactly I
11:03:22 mean by a "signature-based detection method." And the
11:03:26 problem is that there is an uneven meaning to this
11:03:32 expression in the literature. And so I'm reluctant to
11:03:34 express an opinion about that.
11:03:37 The fact is that there may be some attacks
11:03:44 when I'm three standard deviations away from the
11:03:50 baseline mean that definitely connotes an attack, and
11:03:54 it can't be innocuous traffic, then sure, what you
11:03:58 essentially have is a statistical story, and it yields
11:04:03 a signature, I'm certain, I sound an alert, and I am
11:04:03 absolutely certain that there is an attack in play.
11:04:06 BY MS. MOEHLMAN:
11:04:08 Q. What is your understanding of what the
11:04:13 patent specification -- of how the patent
specification uses the term "signature-based

Page 65

11:04:17 technique"?
11:04:23 A. I think that the patent, for example, in
11:04:33 referring to, you know, failed login attempts or
11:04:37 pings, and I'm misremembering where in the patent it
11:04:44 mentions this, but a classic example of what the
11:04:47 patent would call and what's typically called in the
11:04:51 literature a signature-based detection rule is three
11:04:54 failed login attempts. And that's know as a
11:04:54 signature-based rule.
11:05:05 But the truth is that there's two elements to
11:05:06 this. The first is that the fact that a packet to a
11:05:10 network monitor will be participating in a failed
11:05:13 login attempt may not be evident. So that, in a
11:05:17 sense, is the kind of thing that a network monitor may
11:05:20 not -- may have to infer. It may not actually know.
11:05:24 It's more like what a host-based monitor may know,
11:05:28 what a network monitor may have to infer for lack of
11:05:30 detailed information as to what this packet is
11:05:31 actually trying to do.
11:05:34 But three failed login attempts may be an
11:05:40 attack or the start of an attack. It may be just an
11:05:42 accidental thing. But it's typically referred to as a
11:05:45 signature of something suspicious. So it's one of
11:05:47 those gray areas where you're talking about something
statistical. It may actually be even likely that

Page 94

11:55:32 if there is a legal reading of claim 10. But the way
11:55:36 I understand claim 10 is that in addition to deploying
11:55:41 network monitors in a particular domain, you're also
11:55:46 deploying a hierarchical monitor in that domain.
11:55:48 That's the way I read it. I'm not sure legally what
11:55:48 the standard is.
11:55:50 MS. MOEHLMAN:
11:55:53 Q. Do you agree or disagree with SRI's proposed
11:56:02 construction of network monitor?
11:56:06 A. I had a hand in these constructions, so I
11:56:12 would agree. It's the first --
11:56:18 Q. And in SRI's construction of network
11:56:21 monitor, at the end it says, "Service monitors,
11:56:25 domain monitors and enterprise monitors are examples
11:56:27 of network monitors." Do you see that?
11:56:28 A. Mm-hmm.
11:56:39 Q. Do you agree with that?
11:56:39 MR. POLLACK: Objection. Vague and
11:56:57 ambiguous.
11:56:59 THE WITNESS: I think the key thing there is
11:57:06 depending on the context of the specific claim. In
11:57:14 the context of the -- of this claim 1, and my plain
11:57:14 reading of it, I wouldn't change my previous answer.
11:57:21 BY MS. MOEHLMAN:
Q. So do you --

11:57:25 A. So in the context of some claims, it may be
11:57:28 that domain monitors are referred to as network
11:57:39 monitors. But in this specific claim, I think that
11:57:47 this definition of network monitor is rather more
11:57:52 generic. My reading, literal reading of the claim is
11:57:56 that in the second element, the detecting element of
11:58:01 claim 1, the network monitor looks at packet traffic
11:58:07 and generates reports of suspicious activity. For
11:58:11 this specific claim, the hierarchical monitor receives
11:58:14 reports of suspicious activity. My understanding of
11:58:24 the dependent claim 10 is that if all you were doing
11:58:28 was deploying network monitors in the domain, you
11:58:32 wouldn't need the dependent claim 10. So --
11:58:38 Q. Is it your understanding that claim terms
11:58:54 can be construed differently in different claims?
11:59:07 A. Well, certainly not in the same patent.
11:59:11 Q. So let me go back to my original question
11:59:14 where under the joint claims construction statement
11:59:19 that has been marked as Kesidis Exhibit 8, where it
11:59:25 states, "Service monitors, domain monitors and
11:59:28 enterprise monitors are examples of network
11:59:30 monitors," do you agree with that construction, or do
11:59:33 you disagree with that construction?
11:59:36 MR. POLLACK: Objection. Asked and answered,
argumentative.

Page 96

11:59:48 THE WITNESS: Well, in the sense that I agree
11:59:53 with the construction in a generic sense that these
11:59:58 are both network monitors and hierarchical monitors,
12:00:02 by which I also include domain monitors in the context
12:00:06 of '615, they're ultimately examining, directly
12:00:13 examining packet traffic or reports or event streams
12:00:13 generated by packet traffic, network traffic data.
12:00:23 BY MS. MOEHLMAN:
12:00:25 Q. Do you disagree with it in any sense?
12:00:25 MR. POLLACK: Objection.
12:00:35 THE WITNESS: I think that the domain monitor
12:00:39 in this case is -- in my opinion, the domain monitor
12:00:45 is something different from a network monitor. It's
12:00:51 something that's instead of looking at packet traffic,
12:00:54 it's looking at reports of suspicious activity in the
12:00:54 domain. That's the way I read claim 10.
12:01:01 BY MS. MOEHLMAN:
12:01:05 Q. Separate and apart from the claim 10 --
12:01:08 A. It's in -- you know, called out in this more
12:01:11 generic definition of network monitor, I see a domain
12:01:15 monitor is different from the network monitor, the
12:01:18 specific kind of network monitor that's in play in the
12:01:22 detecting element. So as I see this claim
12:01:26 construction, there are different kinds of quote,
unquote network monitors. And in the independent

Page 97

12:01:36 claim '615 claim 1, in the detecting element, the
12:01:41 network monitor is something that is examining packet
12:01:45 data and creating reports of suspicious activity.

12:01:48 Q. So it is your opinion that the network
12:01:51 monitor called out in claim 1 is not a domain
12:01:52 monitor?

12:01:58 A. I think that the network monitor called out
12:02:00 in claim 1 is -- yeah, is not a domain monitor.
12:02:05 That's called out in Claim 10.

12:02:08 Q. And is it your opinion that the network
12:02:13 monitor called out in claim 1 is not an enterprise
12:02:13 monitor?

12:02:16 A. The network monitor is not an enterprise
12:02:17 monitor, no.

12:02:20 Q. Do you understand by this element in claim 1
12:02:26 that the network monitor needs to receive network,
12:02:27 raw network traffic data?

12:02:35 MR. POLLACK: Okay. Vague and ambiguous.

12:02:35 THE WITNESS: The network monitoring called
12:02:35 out in claim 1 says, "suspicious network activity
12:02:36 based on analysis" --

12:02:37 (Reporter interruption.)

12:02:38 THE WITNESS: Sorry. I'm just reading
12:02:41 detecting element, "suspicious network activity based
on an analysis of network traffic data."

Page 194

16:01:36 the actual execution, the branch is taken by the
16:01:39 finite state machine that's running OSPF, for example,
16:01:43 and the entries in the routing information base, and
16:01:47 you're able to observe that, and you have a model of
16:01:50 it, as well, and you're saying, okay, I'm making a
16:01:54 judgment. This is an abnormal branch; this is a
16:01:57 normal branch. That kind of very detailed, very
16:02:01 sophisticated kind of protocol anomaly detection is
16:02:04 not possible in a network intrusion detection, in a
16:02:05 network sensor.

16:02:08 Q. What is disclosed in the patent exactly that
16:02:12 allows you to address the problems associated with
16:02:16 detecting intrusions in larger networks?

16:02:26 MR. POLLACK: Objection. Overbroad, vague
16:02:26 and ambiguous.

16:02:28 THE WITNESS: So to respond to that, I would
16:02:32 simply enunciate the broad design principles or design
16:02:43 objectives of the invention, and that is that the
16:02:52 hierarchy, the lowest level at the network service
16:02:57 monitor, in the jargon of the patents, to take this
16:03:03 torrent of information and create an intermediate
16:03:08 event list that the Markush group speaks to, and from
16:03:17 that, create reports of suspicious activity and then
16:03:20 communicate only those reports to the upper level of
the hierarchy. So what you have is a hierarchy, and

Page 195

16:03:30 you have -- each element of the hierarchy is very
16:03:34 judicious in the amount of computation it does and the
16:03:42 volume of communication that it sends up the ladder.
16:03:45 And I think those kinds of considerations are
16:03:50 simply not in play in NIDES and JiNao. And as a
16:03:55 result, the statistical techniques, specific
16:04:00 statistical techniques you use on the different kinds
16:04:09 of data that you're considering in a NIDS -- a network
16:04:13 intrusion detection system as opposed to a host-based
16:04:15 intrusion detection system are just that: They're
16:04:16 different.

16:04:18 MS. MOEHLMAN: We need to change the tape, so
16:04:20 we need to take a break.

16:04:22 THE WITNESS: Oh, I'm sorry.

16:04:23 THE VIDEOGRAPHER: We're going off the
16:04:29 record. The time is 4:04 p.m. This marks the end of
16:04:37 tape number 3 in the deposition of George Kesidis.

16:18:21 (Break taken from 4:04 to 4:18 p.m.)

16:18:22 THE VIDEOGRAPHER: We're back on the record.
16:18:25 The time is 4:18 p.m. This marks the beginning of
16:18:25 tape No. 4 in the deposition of George Kesidis.

16:18:33 BY MS. MOEHLMAN:

16:18:40 Q. Now, you've read a little bit of the
16:18:42 RealSecure prior art, have you not?

A. Right.

UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation,

Plaintiff and
Counterclaim-Defendant,
vs. NO: 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation; and SYMANTEC
CORPORATION, a Delaware corporation,
Defendants and
Counterclaim-Plaintiffs.
_____________________________________/

DEPOSITION OF GEORGE KESIDIS
VOLUME II

DATE: Friday, May 26, 2006
TIME: 9:00 A.M.
LOCATION: DAY, CASEBEER, MADRID & BATCHELDER
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014

REPORTER: Patricia Hope Sales, CRR
CSR License Number C-4423

BELL & MYERS
Certified Shorthand Reporters, Inc.
50 AIRPORT PARKWAY, SUITE 205
SAN JOSE, CALIFORNIA 95110
Telephone: (408) 287-7500 Fax: (408) 294-1211

Page 283

claim is referring to a -- an interface between a -- say, a third-party network service monitor to the hierarchical monitor. That is to say, an interface between a network service monitor of one vendor and a hierarchical monitor of another, allowing the network service monitor to meaningfully communicate to the hierarchical monitor for the purposes of -- of detection as described in the independent claim.

Q. What about an API to the network monitor?

MR. POLLACK: Objection. Vague and ambiguous.

BY MS. MOEHLMAN:

Q. Well, let me ask you again: You disting- -- you don't -- you do not believe that the network monitors of claim one are also hierarchical monitors; is that right?

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation.

THE WITNESS: I -- the network monitors used in the deploying element of claim one are in my opinion what the spec calls "network service monitors." And the reason why I say that is implicitly in the detecting step, the -- they are looking at network traffic data directly.

BY MS. MOEHLMAN:

Q. Okay. So --

Page 284

A. Whereas the hierarchical monitors implicitly in the automatically receiving step element are looking only at reports of suspicious activity.

Q. Okay. So now let's go to claim four where it says "wherein the plurality of network monitors," right?

And by that you are interpreting "network monitors" from claim one to be network service monitors?

A. That -- that's correct.

Q. Okay.

A. Yeah.

Q. It says, "The plurality of network monitors include an API for encapsulation of monitor functions."

What is that API for encapsulation of monitor functions as to the network service monitors?

MR. POLLACK: Objection. Asked and answered, vague and ambiguous.

THE WITNESS: I -- I believe that -- I believe this claim is -- is modifying the deploying step of the independent claim to in- -- include on the one hand, for example, modifying the deploying set (sic) of the -- of the --

(Reporter clarification.)

THE WITNESS: Sorry.

Page 285

-- for -- modifying the deploying step of the independent claim, for example, so as to include network monitors from different vendors that may generate reports of suspicious activities in -- in different formats, and in this case adding an interface so as -- an interface that -- that, for example, is -- is able to simply translate reports of -- of suspicious activity from one vendor that are interpretable by the -- by the hierarchical monitor -- a hierarchical monitor of another vendor.

So they are I believe identifying other objects or processes called "APIs" that are part of the deploying step.

BY MS. MOEHLMAN:

Q. You don't read this as requiring that the network service monitors include an API?

MR. POLLACK: Objection. Vague and ambiguous.

THE WITNESS: You mean whether the API is a necessary part of the network service monitor?

BY MS. MOEHLMAN:

Q. Yes.

A. I -- I don't really -- I don't really read that specific limitation in the literal language of the claim. I -- it's the first time I have considered the question with regard to this claim, and "the plurality

Page 286

includes," and so it could be that this claim would be satisfied if there was an API deployed in the network monitor, or it could be that the API is a separate -- is a separate process or apparatus included in the plurality.

I'm not sure that -- just reading the language of the claim with your question in mind for the first time, that necessarily it implies that the network monitor itself -- each -- each third-party network monitor needs to include an API.

Q. That -- that wasn't the question.

A. I'm sorry.

Q. Okay? Do you -- you read the language that says "wherein the plurality of network monitors," right? It says "wherein." It's talking about the plurality of network monitors --

A. Right.

Q. -- identified in claim one. You understand that, correct?

A. Um-hmm.

Q. Okay. And it says "network monitors include." Do you read that language to mean that what follows is going to be part of the network monitors that were referenced in claim one?

MR. POLLACK: Objection. Asked and answered,

Page 328

A. The automatically receiving it?

The -- the kind of combination conducted by ISS, that is to say, merely displaying the events at a same console, is -- is not in my opinion what was meant by "integration" in the claim.

So I -- I'm assuming that if simply displaying the events as received is construed to be integrating, then I would agree that the -- the "automatically" element would be -- would be met, but I -- I didn't really -- haven't really thought about it too carefully.

Q. Is it your opinion that the RealSecure console in the prior art merely displayed the events as received?

MR. POLLACK: Objection. Lacks foundation, vague and ambiguous.

THE WITNESS: I believe that for purposes of brevity, that largely identical reports were -- were grouped together for visualization purposes.

BY MS. MOEHLMAN:

Q. And by grouping them together, would you consider that to be combining reports received?

MR. POLLACK: Objection. Vague and ambiguous.

THE WITNESS: Given a -- a plain meaning of the word "combining," sure.

UNITED STATES DISTRICT COURT

DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC.,
a California corporation

Plaintiff and
Counterclaim-Defendant,

vs. No. 04-1199 (SLR)

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation; and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs./

DEPOSITION OF GEORGE KESIDIS

VOLUME III

DATE: May 29, 2006

TIME: 9:00 a.m.

LOCATION: DAY CASEBEER MADRID & BATCHELDER
20300 Stevens Creek Boulevard
Suite 400
Cupertino, CA 95014

REPORTED BY: KAREN L. BUCHANAN
CSR No. 10772

statistical technique.

BY MR. GALVIN:

Q. How could a -- withdraw that.

In a statistical technique, would the threshold be empirically determined based on observed activity as opposed to being preset?

MR. POLLACK: Objection. Vague and ambiguous, lacks foundation.

THE WITNESS: I think certainly if it's -- certainly if it's based on empirical activity, it may be hard to classify a particular technique, if the threshold is based on empirical activity as signature. However, if it's not, again, it's one of those gray areas I mentioned earlier, depending on the information that's in play against which you're comparing the threshold, I could see it as being a signature approach or a statistical approach.

BY MR. GALVIN:

Q. If a person skilled in the art was trying to determine whether certain activity or a certain technique that they wanted to add to their intrusion detection system fell within the scope of the claims of the SRI patents, particularly, let's say, claim 1 of the '212 patent, how would they be able to determine whether this particular technique using thresholds fell with -- inside the scope of the claim or outside the scope of the claim?

MR. POLLACK: Objection. Vague and ambiguous, incomplete hypothetical.

THE WITNESS: Pardon me. I just want to put claim 1 of the '212 in front of me.

I would answer that in the context of this paragraph in column 7 of the '338 patent by, for example, pointing out that I don't think that the input information is the same as what's implicitly in play in the claims for '212, necessarily in play. I think with reference to statistical detection methods, I think that the kinds of information you're building based on observed network traffic data, the kinds of measures you're taking, such as those listed in the Markush groups of other claims, in and of themselves, the individual packets may be completely innocuous, whereas -- and that really means that the kinds of detections that you -- the kinds of detection techniques that you create using that information tend to be much more statistical in nature than, for example, observing failed login request and saying after three failed login requests, I'm going to trip an alert. I would refer to the latter as a more signature-based approach -- I'm sorry, as a kind of

activity.

BY MR. GALVIN:

Q. Let's stick with the failed logins. So I take it you would agree, based on the specification, that a technique that identifies suspicious activity by setting a threshold, let's say three failed logins, would be a signature detection technique?

MR. POLLACK: Objection. Vague and ambiguous.

THE WITNESS: It's what the patent would -- again, reading column 7, it's what the patent specification would call a rudimentary, inexpensive signature analysis technique that involves a threshold.

BY MR. GALVIN:

Q. And in -- that example would not be a statistical detection method, correct?

MR. POLLACK: Objection. Vague and ambiguous.

THE WITNESS: If it's generating a report as a result of the three failed login attempts and calling that report a report of suspicious activity, it would not be termed a statistical method, right.

BY MR. GALVIN:

Q. Now, suppose instead of just counting the three failed logins, suppose I decided to set a threshold that stated if the number of failed logins exceeds 5 percent of the total number of logins in a given period of time, I will flag that as suspicious activity. Is that a statistical detection method or a signature detection method?